

SEC. 1296. REPORT ON CERTAIN ENTITIES CONNECTED TO FOREIGN PERSONS ON THE MURDER OF JAMAL KHASHOGGI.

(a) **IN GENERAL.**—Not later than 180 days after the date of the enactment of this Act, the Secretary of State, in consultation with the heads of appropriate agencies, shall submit to the appropriate congressional committees a report on private, commercial, and nongovernmental entities, including nonprofit foundations, controlled in whole or in part by any foreign person named in the Office of the Director of National Intelligence report titled “Assessing the Saudi Government’s Role in the Killing of Jamal Khashoggi”, dated February 11, 2021.

(b) **MATTERS TO BE INCLUDED.**—The report required by subsection (a) shall include the following:

(1) A description of such entities.

(2) A detailed assessment, based in part on credible open sources and other publicly-available information, of the roles, if any, such entities played in the murder of Jamal Khashoggi or any other gross violations of internationally recognized human rights.

(3) A certification of whether any such entity is subject to sanctions pursuant to the Global Magnitsky Human Rights Accountability Act (22 U.S.C. 2656 note).

(c) **FORM.**—The report required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

(d) **APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.**—In this section, the term “appropriate congressional committees” means—

(1) the Committee on Foreign Affairs and the Permanent Select Committee on Intelligence of the House of Representatives; and

(2) the Committee on Foreign Relations and the Select Committee on Intelligence of the Senate.

SA 4240. Mr. MENENDEZ (for himself, Mr. RUBIO, Mr. MERKLEY, and Mr. COONS) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle E of title XII, add the following:

SEC. 1253. SAFE HARBOR FOR HONG KONG REFUGEES.

(a) **DESIGNATION OF CERTAIN RESIDENTS OF HONG KONG AS PRIORITY 2 REFUGEES.**—

(1) **IN GENERAL.**—The Secretary of State, in consultation with the Secretary of Homeland Security, shall designate, as Priority 2 refugees of special humanitarian concern, the following categories of aliens:

(A) Individuals who are residents of the Hong Kong Special Administrative Region who suffered persecution, or have a well-founded fear of persecution, on account of their peaceful expression of political opinions or peaceful participation in political activities or associations.

(B) Individuals who have been formally charged, detained, or convicted on account of their peaceful actions as described in section 206(b)(2) of the United States-Hong Kong Policy Act of 1992 (22 U.S.C. 5726).

(C) The spouses, children, and parents (as such terms are defined in subsections (a) and (b) of section 101 of the Immigration and Na-

tionality Act (8 U.S.C. 1101)) of individuals described in subparagraph (A) or (B), except such parents who are citizens of a country other than the People’s Republic of China.

(2) **PROCESSING OF HONG KONG REFUGEES.**—The processing of individuals described in paragraph (1) for classification as refugees may occur in Hong Kong or in a third country.

(3) **ELIGIBILITY FOR ADMISSION AS REFUGEES.**—An alien may not be denied the opportunity to apply for admission as a refugee under this subsection primarily because such alien—

(A) qualifies as an immediate relative of a citizen of the United States; or

(B) is eligible for admission to the United States under any other immigrant classification.

(4) **FACILITATION OF ADMISSIONS.**—An applicant for admission to the United States from the Hong Kong Special Administrative Region may not be denied primarily on the basis of a politically motivated arrest, detention, or other adverse government action taken against such applicant as a result of the participation by such applicant in protest activities.

(5) **EXCLUSION FROM NUMERICAL LIMITATIONS.**—Aliens provided refugee status under this subsection shall not be counted against any numerical limitation under section 201, 202, 203, or 207 of the Immigration and Nationality Act (8 U.S.C. 1151, 1152, 1153, and 1157).

(6) **REPORTING REQUIREMENTS.**—

(A) **IN GENERAL.**—Not later than 180 days after the date of the enactment of this Act, and every 90 days thereafter, the Secretary of State and the Secretary of Homeland Security shall submit a report regarding the matters described in subparagraph (B) to—

(i) the Committee on the Judiciary and the Committee on Foreign Relations of the Senate; and

(ii) the Committee on the Judiciary and the Committee on Foreign Affairs of the House of Representatives.

(B) **MATTERS TO BE INCLUDED.**—Each report required under subparagraph (A) shall include—

(i) the total number of applications that are pending at the end of the reporting period;

(ii) the average wait-times for all applicants who are currently pending—

(I) employment verification;

(II) a prescreening interview with a resettlement support center;

(III) an interview with U.S. Citizenship and Immigration Services; or

(IV) the completion of security checks; and

(iii) the number of denials of applications for refugee status, disaggregated by the reason for each such denial.

(C) **FORM.**—Each report required under subparagraph (A) shall be submitted in unclassified form, but may include a classified annex.

(D) **PUBLIC REPORTS.**—The Secretary of State shall make each report submitted under this paragraph available to the public on the internet website of the Department of State.

(7) **SATISFACTION OF OTHER REQUIREMENTS.**—Aliens granted status under this subsection as Priority 2 refugees of special humanitarian concern under the refugee resettlement priority system shall be considered to satisfy the requirements under section 207 of the Immigration and Nationality Act (8 U.S.C. 1157) for admission to the United States.

(b) **WAIVER OF IMMIGRANT STATUS PRESUMPTION.**—

(1) **IN GENERAL.**—The presumption under the first sentence of section 214(b) of the Immigration and Nationality Act (8 U.S.C.

1184(b)) that every alien is an immigrant until the alien establishes that the alien is entitled to nonimmigrant status shall not apply to an alien described in paragraph (2).

(2) **ALIEN DESCRIBED.**—

(A) **IN GENERAL.**—An alien described in this paragraph is an alien who—

(i) is a resident of the Hong Kong Special Administrative Region on February 8, 2021;

(ii) is seeking entry to the United States to apply for asylum under section 208 of the Immigration and Nationality Act (8 U.S.C. 1158); and

(iii)(I) had a leadership role in civil society organizations supportive of the protests in 2019 and 2020 relating to the Hong Kong extradition bill and the encroachment on the autonomy of Hong Kong by the People’s Republic of China;

(II) had an organizing role for such protests;

(III) acted as a first aid responder for such protests;

(IV) suffered harm while covering such protests as a journalist;

(V) provided paid or pro-bono legal services to 1 or more individuals arrested for participating in such protests; or

(VI) during the period beginning on June 9, 2019, and ending on February 8, 2021, was formally charged, detained, or convicted for his or her participation in such protests.

(B) **EXCLUSION.**—An alien described in this paragraph does not include any alien who is a citizen of a country other than the People’s Republic of China.

(c) **REFUGEE AND ASYLUM DETERMINATIONS UNDER THE IMMIGRATION AND NATIONALITY ACT.**—

(1) **PERSECUTION ON ACCOUNT OF POLITICAL OPINION.**—

(A) **IN GENERAL.**—For purposes of refugee determinations under section 207 of the Immigration and Nationality Act (8 U.S.C. 1157), an individual whose citizenship, nationality, or residency is revoked for having submitted to any United States Government agency a nonfrivolous application for refugee status, asylum, or any other immigration benefit under the immigration laws (as defined in section 101(a) of such Act (8 U.S.C. 1101(a))) shall be considered to have suffered persecution on account of political opinion.

(B) **NATIONALS OF THE PEOPLE’S REPUBLIC OF CHINA.**—For purposes of refugee determinations under section 207 of the Immigration and Nationality Act (8 U.S.C. 1157), a national of the People’s Republic of China whose residency in the Hong Kong Special Administrative Region, or any other area within the jurisdiction of the People’s Republic of China, as determined by the Secretary of State, is revoked for having submitted to any United States Government agency a nonfrivolous application for refugee status, asylum, or any other immigration benefit under the immigration laws shall be considered to have suffered persecution on account of political opinion.

(2) **CHANGED CIRCUMSTANCES.**—For purposes of asylum determinations under section 208 of the Immigration and Nationality Act (8 U.S.C. 1158), the revocation of the citizenship, nationality, or residency of an individual for having submitted to any United States Government agency a nonfrivolous application for refugee status, asylum, or any other immigration benefit under the immigration laws shall be considered to be a changed circumstance under subsection (a)(2)(D) of such section.

(d) **STATEMENT OF POLICY ON ENCOURAGING ALLIES AND PARTNERS TO MAKE SIMILAR ACCOMMODATIONS.**—It is the policy of the United States to encourage allies and partners of the United States to make accommodations similar to the accommodations made under this Act for residents of the

Hong Kong Special Administrative Region who are fleeing oppression by the Government of the People's Republic of China.

(e) **TERMINATION.**—This section shall cease to have effect on the date that is 5 years after the date of the enactment of this Act.

SA 4241. Mr. MENENDEZ submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of title XII, add the following:

Subtitle H—Combating International Cybercrime

SEC. 1291. DEFINITIONS.

In this subtitle:

(1) **APPROPRIATE CONGRESSIONAL COMMITTEES.**—The term “appropriate congressional committees” means—

(A) the Committee on Foreign Relations of the Senate;

(B) the Committee on Banking, Housing, and Urban Affairs of the Senate;

(C) the Committee on Foreign Affairs of the House of Representatives; and

(D) the Committee on Financial Services of the House of Representatives.

(2) **CRITICAL INFRASTRUCTURE.**—The term “critical infrastructure” means systems and assets, whether physical or virtual, that are so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating impact on the security, economic security, public health, or safety of the United States.

(3) **CYBERCRIME GROUP.**—The term “cybercrime group” means any group practicing, or which has significant subgroups which practice, international cybercrime.

(4) **INTERNATIONAL CYBERCRIME.**—The term “international cybercrime” means unlawful activities involving citizens, territory, or infrastructure of at least 1 country that is intended—

(A) to disrupt the confidentiality, integrity, or availability of information systems for financial gain or in order to economically benefit a third party;

(B) to damage, delete, deteriorate, alter, or suppress information systems; or

(C) to distribute credentials, access codes, or similar data.

(5) **MAJOR CYBERCRIME INCIDENT.**—The term “major cybercrime incident” means an act of cybercrime, or a series of such acts, that—

(A) results in the death of, or bodily injury to, 1 or more United States citizens;

(B) results in economic loss to United States persons in excess of—

(i) \$5,000,000 in any single act of cybercrime; or

(ii) \$50,000,000 in a series of acts of cybercrime; or

(C) materially disrupts United States critical infrastructure.

(6) **STATE SPONSOR OF INTERNATIONAL CYBERCRIME.**—The term “state sponsor of international cybercrime” means a country, the government of which systematically—

(A) commits international cybercrime;

(B) supports, facilitates, encourages, or expressly consents to international cybercrime by third parties, including contractors, proxies, and affiliates; or

(C) fails to take reasonable steps to detect, investigate, or address cybercrime occurring

within its territory or through the use of its infrastructure.

SEC. 1292. FINDINGS.

Congress finds the following:

(1) Information and communication technologies underpin the prosperity and national security of the United States. However, the widespread use of these technologies also poses serious risks. In particular, cybercrime (criminal activity using digital means) presents an acute and growing threat to the economic, strategic, and security interests of the United States and its allies and partners.

(2) Cybercriminals cause massive harm. According to National Institute of Standards and Technology estimates, in 2016, United States businesses lost between \$167,900,000,000 and \$770,000,000,000 to cybercrime, corresponding to between 0.9 percent and 4.1 percent of the total United States gross domestic product that year. The related risk and harm to public health and safety is incalculable and can only be expected to grow as digital technologies become more intertwined in daily life.

(3) Using a wide variety of tactics, cybercriminals—

(A) steal United States intellectual property and sensitive personal information;

(B) defraud United States businesses and citizens; and

(C) disrupt infrastructure critical to Americans' health and safety.

(4) The use of ransomware (malicious software that encrypts and thereby prevents access to data) until a ransom, often costing millions of dollars, is paid is an especially destructive form of cybercrime.

(5) In 2021, ransomware groups—

(A) crippled or endangered some of the United States' most critical infrastructure, including water utilities, hospitals, meat packing plants, and a critical fuel pipeline; and

(B) extracted hundreds of millions of dollars in ransom from United States businesses and their insurers.

(6) United States allies and partners have also suffered major losses from cybercrime. Recent ransomware victims include Swedish supermarkets, Ireland's national health service, a leading European insurer, and a major German chemical manufacturer.

(7) The Council of Europe's Convention on Cybercrime, done at Budapest November 23, 2001, states, “an effective fight against cybercrime requires increased, rapid and well-functioning international cooperation in criminal matters” and requires parties to outlaw digital fraud, digital forgery, intellectual property theft through digital means, and offenses against confidentiality, integrity, and availability of computer data and systems, among other misconduct.

(8) In July 2021, the United Nations Group of Governmental Experts on Advancing responsible State behavior in cyberspace, which includes experts from the United States, Russia, and China, issued a report stating that countries are expected to “take all appropriate and reasonably available and feasible steps to detect, investigate and address” known cybercriminal activity emanating from within their borders.

(9) Certain nations, including China, Russia, Iran, and North Korea, ignore, facilitate, or directly participate in cybercrime as a matter of national policy.

(10) Russia is a global haven for cybercriminals, including ransomware groups responsible for attacks on fuel pipelines, meat packing plants, and supermarkets in the United States and in Europe in 2021. These gangs operate freely and with the Kremlin's tacit approval. By allowing cybercriminals to operate with impunity,

Russia threatens international stability, undermines international institutions, and disregards international norms.

(11) The People's Republic of China uses cybercrime—

(A) to undermine United States' interests; and

(B) to victimize United States' businesses and government agencies.

(12) In July 2021, Secretary of State Blinken stated, “The PRC's Ministry of State Security (MSS) has fostered an ecosystem of criminal contract hackers who carry out both state-sponsored activities and cybercrime for their own financial gain. ... These contract hackers cost governments and business billions of dollars in stolen intellectual property, ransom payments, and cybersecurity mitigation efforts, all while the MSS has them on its payroll.”

(13) Cybercrime is central to North Korea's geopolitical strategy, helping the Kim Jong Un regime maintain its grip on power and providing essential resources for the country's nuclear weapons program.

(14) In February 2021, the Department of Justice indicted 3 North Korean military intelligence agents for a “wide-ranging criminal conspiracy to conduct a series of destructive cyberattacks, to steal and extort more than \$1.3 billion of money and cryptocurrency from financial institutions and companies, to create and deploy multiple malicious cryptocurrency applications, and to develop and fraudulently market a blockchain platform.”

(15) North Korean hackers are responsible for many of the most brazen cybercrime campaigns, including—

(A) the 2017 WannaCry global ransomware incident;

(B) the 2014 cyberattack on Sony Pictures; and

(C) the attempted theft of nearly \$1,000,000,000 from the Central Bank of Bangladesh in 2016.

(16) The Iranian regime is a prolific sponsor of cybercrime. Hackers linked to Iran's Islamic Revolutionary Guard Corps target businesses, academic institutions, and research organizations around the world.

(17) In 2018, the Department of Justice indicted 9 Iranians for a coordinated campaign of cyber intrusions into computer systems belonging to 144 United States universities, 176 universities across 21 foreign countries, 47 domestic and foreign private sector companies, the Department of Labor, the Federal Energy Regulatory Commission, the State of Hawaii, the State of Indiana, the United Nations, and the United Nations Children's Fund.

SEC. 1293. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) all nations must take reasonable steps to stop cybercriminal activities from taking place within their territories or through their infrastructure;

(2) governments that tolerate, facilitate, or participate in cybercrime threaten the economic and national security of the United States, United States allies and partners, and the international community; and

(3) the rising threat of international cybercrime requires a robust, coordinated response from the United States Government, United States allies and partners, and the private sector—

(A) to prevent and counter international cybercriminal activity; and

(B) to impose significant and tangible costs on cybercriminal groups and on governments that tolerate, facilitate, or participate in cybercrime.

SEC. 1294. STATEMENT OF POLICY.

It shall be the policy of the United States—